

**GOV** Government

**C** Computer  
**E** Emergency  
**R** Response  
**T** Team

**.NL** The Netherlands



GOV<img alt="globe icon" data-bbox="625 755 655 790"/>CERT.NL



---

# Monitoring threats and vulnerabilities

---

*Taranis*

---

## Monitoring threats & vulnerabilities (1)



12x7 active duty



24x7 available for handling ICT security incidents

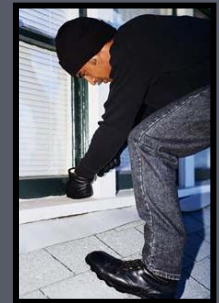


Monitoring of open and closed sources

- Websites
- Honey pots
- Other CERT's
- Mailing lists
- IRC



Handle reports send to [cert@govcert.nl](mailto:cert@govcert.nl)



## Monitoring threats & vulnerabilities (2)



Writing security advisories for our constituency (government)



Writing a weekly overview of security news ('End-of-Week')



Alerting citizens and small business through [Waarschuwingsdienst.nl](http://Waarschuwingsdienst.nl)



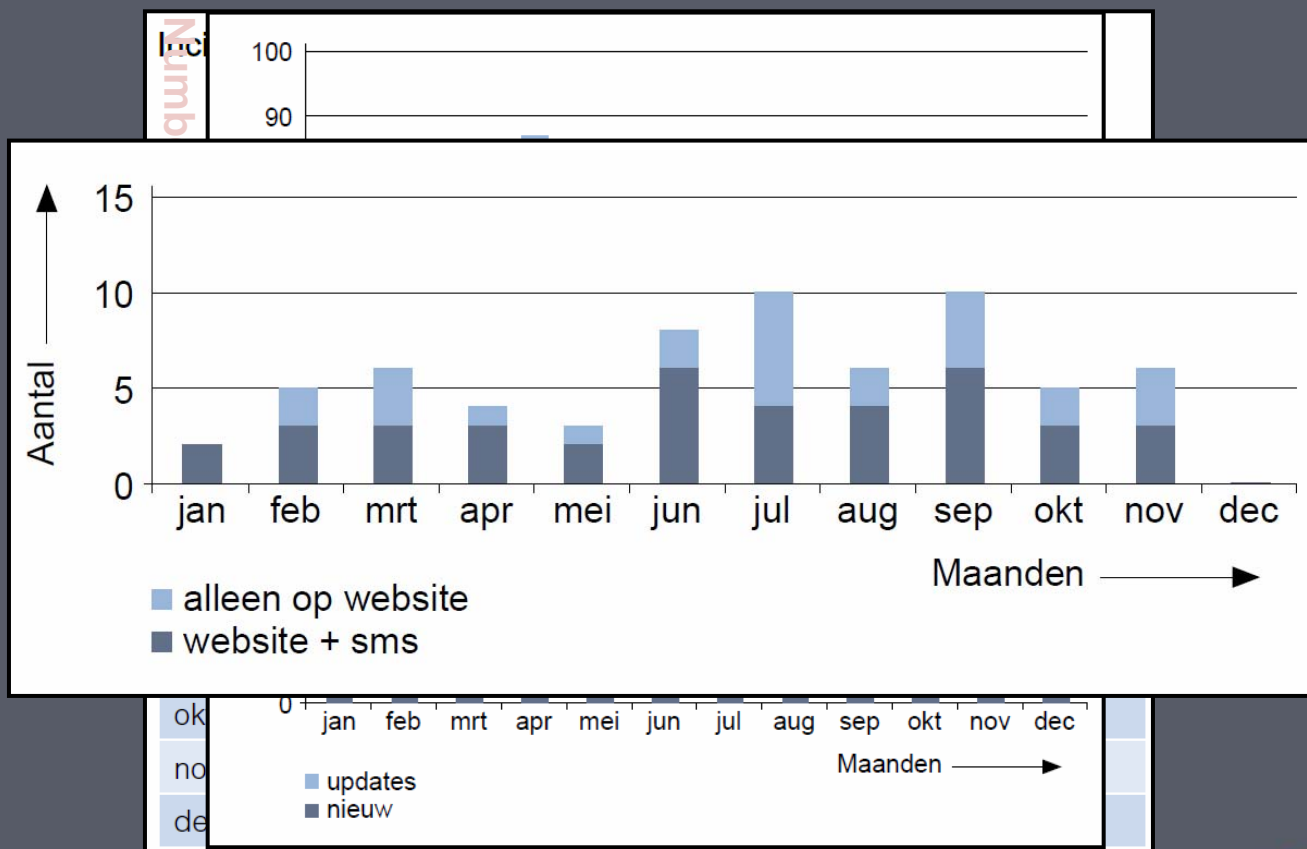
Informing colleagues through an internal mailing list



Weekly circulation (9 persons)

## Monitoring threats & vulnerabilities (3)

Number of alerts WD.NL

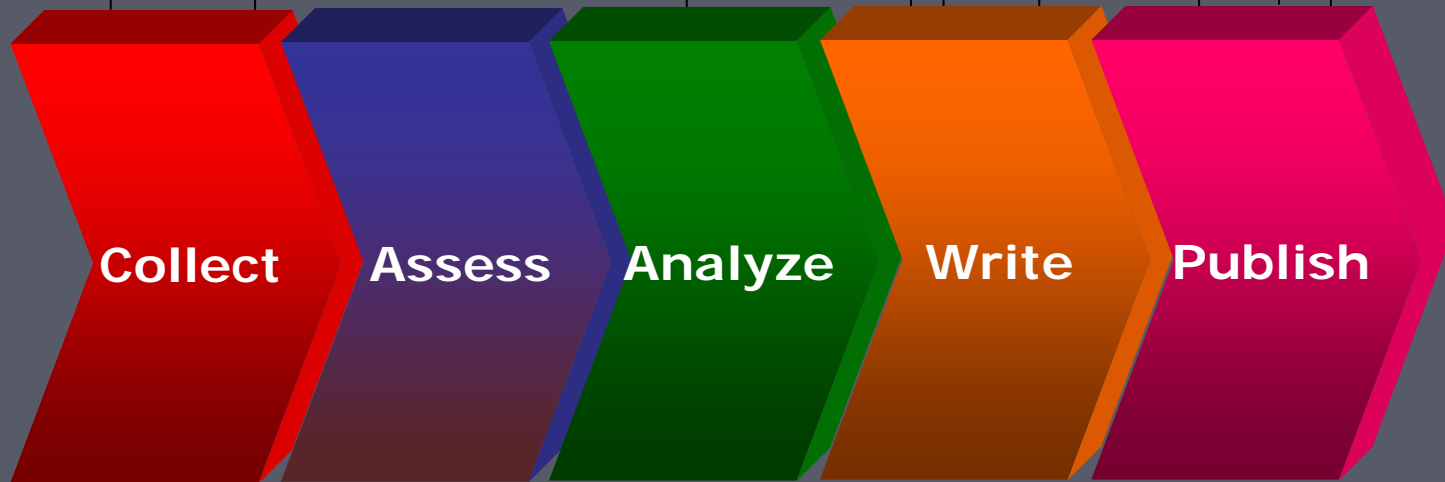
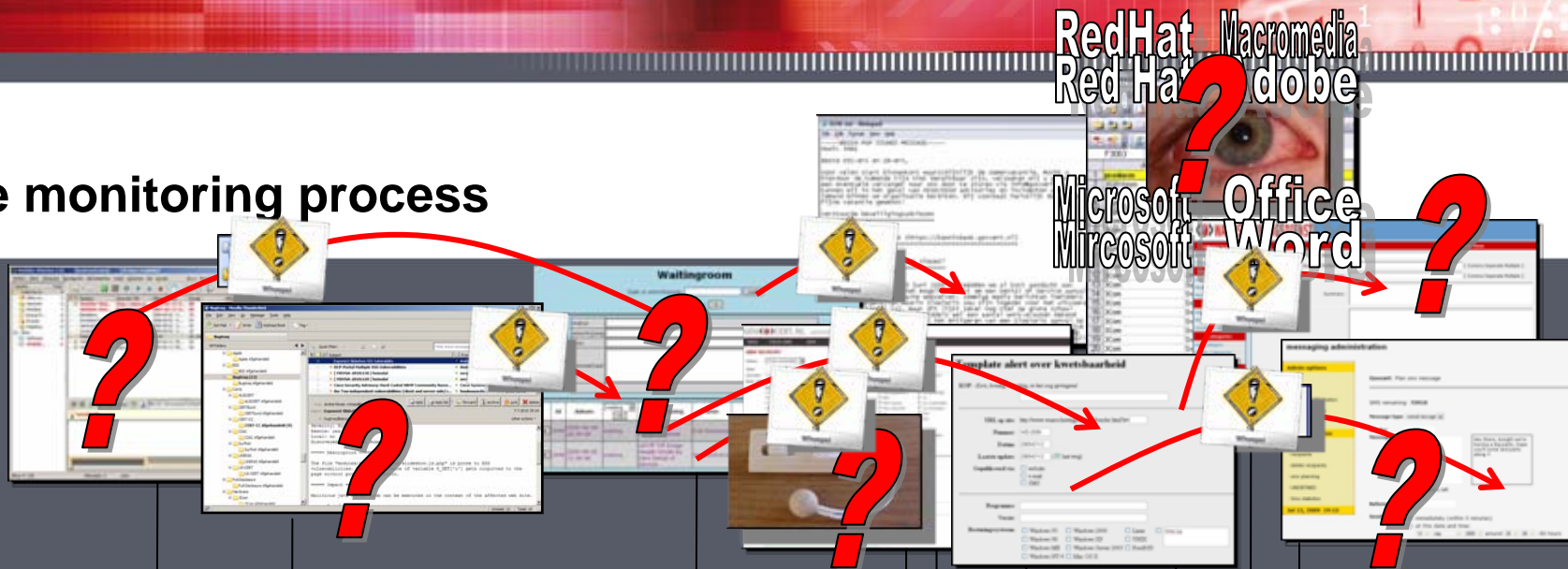




## The monitoring process



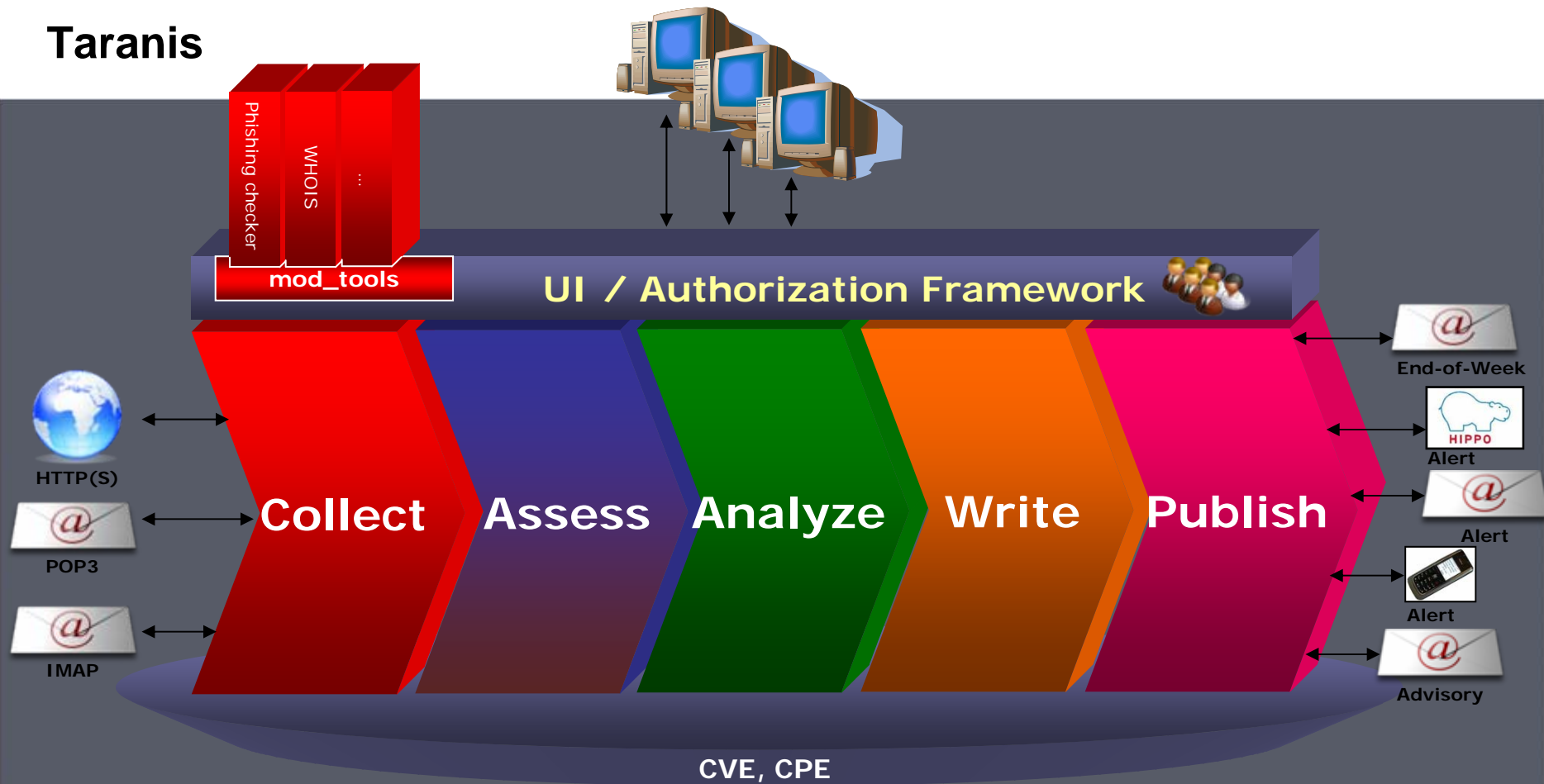
# The monitoring process

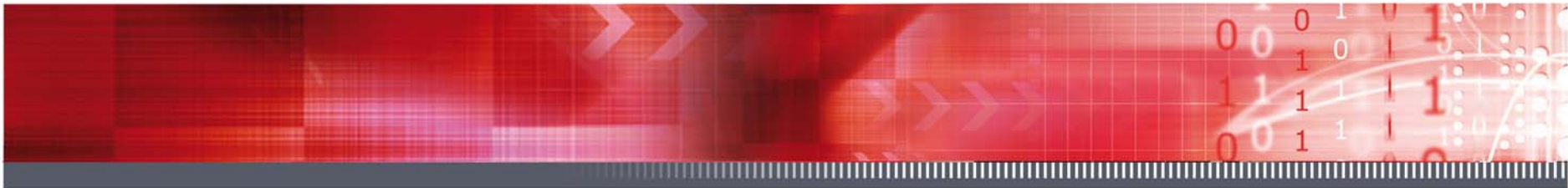


## Taranis principles

- Integration of all phases into one tool
- Minimal 'copy-and-paste' actions
- Higher efficiency, lower error rates
- Use of templates for standard texts
- Taranis as the source for advisories, alerts and End-of-Weeks
- Modular composition
- Sharing with the community
- Traceability of actions

# Taranis





Home > [Risico's](#) > [Actuele dreigingen](#) > [Softwarelekken](#) > WD-2010-057  
Google Chrome update verhelpt diverse lekken

# Taranis products

## Google Chrome update verhelpt diverse

Dreiging

from GOVCERT.NL <cert@govcert.nl>★  
subject GOVCERT.NL-2010-227 [v1.02] [L/M] Mee  
to advisory-XML@lists

from GOVCERT.NL <cert@govcert.nl>★  
subject [govcert.nl #994] Phishing activity at hXXp://  
to abuse@  
bcc rt@tickets.govcert.nl★

Statistics type  
Advisories by classificatie

|            |      |
|------------|------|
| Start date | End  |
| 01-06-2010 | 31-0 |

Statistics

-----BEGIN PGP S  
Hash: SHA1

-----BEGIN PGP SIGNED MESSAGE-----  
Hash: SHA1

#####  
## G O V C E R T . N L  
#####

Dear abuse,

Titel  
Advisory ID  
Versie  
Kans  
CVE ID

On behalf of GOVCERT.NL, I would like to request your assistance. GOVCERT.NL is the Computer Emergency Response Team for the Dutch Government.

Schade

We have received a report of phishing activity against a large Dutch bank. The phishing site is located at hXXp:// Details of the phishing website:

Auteur  
Uitgiftedatum  
Toepassing  
Versie(s)  
Platform(s)

URL:  
hXXp:// /home2.php  
(link modified for security reasons)

Beschikbaarheid

This web address resolves to .6, for which you are listed as the abuse contact.

Update

Fedora heeft  
voor Fedora 1

WHOIS:

| AS    | IP | CC | AS Name |
|-------|----|----|---------|
| 10297 | .6 | US |         |

Samenvatting

Twee kwetsbaar  
om willekeurige code u  
veroorzaken op een app

We kindly ask you to investigate this matter and to take appropriate action. Any feedback of your actions is highly appreciated. Many thanks in advance for your help.

Kind regards,

[Home](#)

Windows  
OS X

accounts and  
ted for 42 of






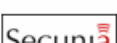
De nieuwste versie  
rschuwingsdienst.nl  
chrome automatisch  
atie te installeren

# Demo

GOV<img alt="Globe icon" data-bbox="435 385 455 405"/>CERT.NL edum: ST medewerker |  search | [Advanced search](#)

ASSESS ANALYZE WRITE PUBLISH CONFIGURATION TOOLS STATISTICS LOGOUT Switch to custom search

Category: security-vuln Search:  Start date: 06-07-2010 End date: 06-07-2010 U R I W     Search!

| Timestamp                                    | Source   | Title / description   |   |
|--|--|---|---|
| <input type="checkbox"/> 06-07-2010 14:26:38 |   | <b>i-Net Solution Matrimonial Script alert.php Cross Site Scripting Vulnerability</b><br>2010-07-06             | <input type="button" value="Home"/> <input type="button" value="Download"/> <input type="button" value="Search"/> <input type="button" value="Info"/> |
| <input type="checkbox"/> 06-07-2010 14:04:16 |  | <b>Release of Cacti 0.8.7g Beta 2 and MORE!</b><br>Release of Cacti 0.8.7g Beta 2 and MORE!                     | <input type="button" value="Home"/> <input type="button" value="Download"/> <input type="button" value="Search"/>                                     |
| <input type="checkbox"/> 06-07-2010 13:48:16 |  | <b>Sun Java System Web Server Admin Interface Denial of Service Vulnerability</b><br>2010-07-06                 | <input type="button" value="Home"/> <input type="button" value="Download"/> <input type="button" value="Search"/> <input type="button" value="Info"/> |
| <input type="checkbox"/> 06-07-2010 13:46:08 |  | <b>[webapps] - Pre Multi-Vendor Shopping Malls SQL Injection Vulnerability &amp; Auth Bypass Vulnerability.</b> | <input type="button" value="Home"/> <input type="button" value="Download"/> <input type="button" value="Search"/>                                     |
| <input type="checkbox"/> 06-07-2010 13:29:52 |  | <b>H264WebCam NULL Pointer Dereference PoC</b><br>Target: H264WebCam 3.7 Impact: Denial of service              | <input type="button" value="Home"/> <input type="button" value="Download"/> <input type="button" value="Search"/>                                     |
| <input type="checkbox"/> 06-07-2010 13:28:45 |  | <b>ScriptsFeed Auction Software "id" SQL Injection Vulnerabilities</b><br>Moderately critical                   | <input type="button" value="Home"/> <input type="button" value="Download"/> <input type="button" value="Search"/> <input type="button" value="Info"/> |



## How to obtain the software?

- Sent e-mail to [info@govcert.nl](mailto:info@govcert.nl)
- Sign the Gentlement's Agreement you will receive in return
- After signing you will receive a Software CD and manual



## More information?

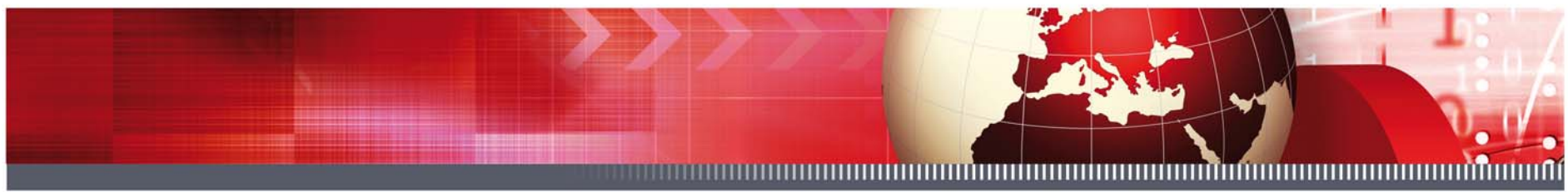
- [contact info@govcert.nl](mailto:contact info@govcert.nl)

- Check our website:

<http://www.govcert.nl/render.html?it=210>

Taranis Workshop organized 17th november (after our symposium)

=> Hands-on class + a chance to meet with the developers



**Thank you for your time!**

**Questions?**